EXHIBIT 7

PRELIMINARY INFRINGEMENT CLAIM CHART

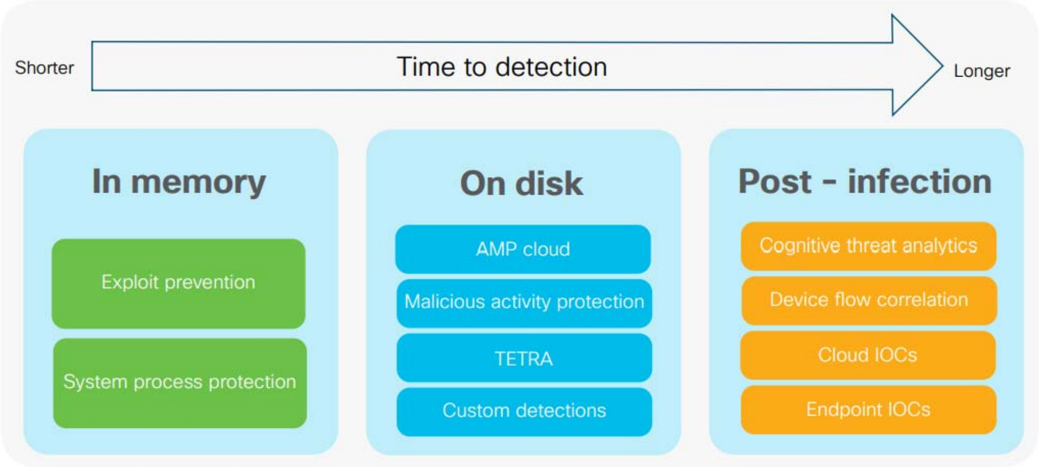
Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;	Cisco Advanced Malware Protection (AMP) includes *a non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information* (e.g., a smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof, including associated information including but not limited to information describing the actual vulnerabilities themselves, information describing endpoints that contain the particular operating system/application/version thereof, information describing policy/detection/remediation techniques for addressing the actual vulnerabilities relevant to the particular operating system/application/version thereof including signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *from at least one first data storage* (e.g., memory on the at least one device storing a repository of the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof, etc.) *that is generated utilizing second vulnerability information* (e.g., a larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof, including associated information including but not limited to information describing the possible vulnerabilities themselves, information describing the different operating systems/applications/versions thereof, information describing policy/detection/remediation techniques for addressing the potential vulnerabilities relevant to the different operating systems/applications/versions thereof including signature/policy updates for anti-virus/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *from at least one second data storage* (e.g., a Common Vulnerabilities and Exposures (CVE) database, etc.) *that is used to identify a plurality of potential vulnerabilities* (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.)*;* **Note**: See, for example, the evidence below (emphasis added, if any):

EXHIBIT 7

PRELIMINARY INFRINGEMENT CLAIM CHART

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	- “AMP Cloud provides access to the global intelligence database that is constantly updated and augmented with new detections and provides a great breadth of knowledge to the AMP Connector through one-to-one hash lookups, a generic signature engine, and the machine learning engine.”  Shorter Time to detection Longer In memory Exploit prevention System process protection On disk AMP cloud Malicious activity protection TETRA Custom detections Post - infection Cognitive threat analytics Device flow correlation Cloud IOCs Endpoint IOCs https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.pdf “**Compromises** By definition, compromises represent potentially malicious activity that has been detected by AMP that has not been quarantined but that may require action on your part. Compromises are displayed through a heat map showing groups with compromised computers and a time graph

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
showing the number of compromises for each day or hour over the past 14 days. Click the <b>Inbox</b> link to view the compromises on the Inbox Tab and take steps to resolve them.”
Cisco <i>AMP for Endpoints User Guide</i>, Chapter 1, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

“<b>Common Vulnerabilities and Exposures</b>

The Common Vulnerabilities and Exposures (CVE) database records known vulnerabilities in various applications. All vulnerabilities are noted by their unique CVE ID. The CVE ID shown in the Console can be clicked to get more details on the vulnerability.”
Cisco <i>AMP for Endpoints User Guide</i>, Chapter 20, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

“Designed for Cisco Firepower® network threat appliances, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.”
https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added)

“<b>Features and Benefits of Cisco AMP for Endpoints</b>”

<table>
<tr><th>Feature</th><th>Benefits</th></tr>
<tr><td>. . .</td><td>. . .</td></tr>
<tr><td>Dashboards</td><td>Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td><table>
<tr><td></td><td>information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a comprehensive contextual view so that you can make informed security decisions.</td></tr>
<tr><td>. . .</td><td>. . .</td></tr>
<tr><td>Exploit Prevention</td><td>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes. The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a payload, and zero-day attacks on software vulnerabilities yet to be patched.</td></tr>
<tr><td>. . .</td><td>. . .</td></tr>
<tr><td>Vulnerabilities</td><td>Identify vulnerable software and close attack pathways. This feature shows a list of hosts that contain vulnerable software, a list of the vulnerable software on each host, and the hosts most likely to be compromised. Powered by our threat intelligence and security analytics, AMP identifies vulnerable software being targeted by malware, shows you the potential exploit, and provides you with a prioritized list of hosts to patch.</td></tr>
</table>
https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html
(emphasis added)</td></tr>
<tr><td>said first vulnerability information generated utilizing the second vulnerability information, by:</td><td>Cisco Advanced Malware Protection (AMP) includes <i>said first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>generated utilizing the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating</td></tr>
</table>

Claim 1 Elements	Applicability
identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and	systems/applications/versions thereof)*, by: identifying at least one configuration* (e.g., a Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *associated with a plurality of devices* (e.g., 50+ nodes licensed to use the software, etc.) *including a first device, a second device, and a third device,* (e.g., a first, second, and third of the 50+ nodes licensed to use the software, etc.) *and* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**Vulnerabilities** Vulnerabilities are displayed through a heat map that shows groups that include computers with known vulnerable applications installed." Cisco *AMP for Endpoints User Guide*, Chapter 1, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**Deployment Options for Protection Everywhere** Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:" **Product Name** | **Details**

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Cisco AMP for Endpoints</td><td>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.</td></tr>
</table>
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)

“<b>Software requirements</b>”

<table>
<tr><td>Cisco AMP for Endpoints</td><td>● Microsoft Windows XP with Service Pack 3 or later
● Microsoft Windows Vista with Service Pack 2 or later
● Microsoft Windows 7
● Microsoft Windows 8 and 8.1
● Microsoft Windows 10
● Microsoft Windows Server 2003
● Microsoft Windows Server 2008
● Microsoft Windows Server 2012
● Mac OS X 10.7 and later
● Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3
● Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3</td></tr>
<tr><td>Cisco AMP for Endpoints on Android mobile devices</td><td>Android version 2.1 and later</td></tr>
<tr><td>Cisco AMP for Endpoints on Apple iOS</td><td>MDM supervised iOS version 11</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html "Cisco's AMP for endpoints subscription offerings begin with a minimum of 50 nodes, and thus inherently the network would include a plurality of devices (e.g., nodes, etc.), that include at least a first, second, and third device." http://winncom.com.ua/wp-content/uploads/2018/06/Cisco-Advanced-Malware-Protection-for-Endpoints.pdf
determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;	Cisco Advanced Malware Protection (AMP) includes *determining that the plurality of devices* (e.g., the 50+ nodes licensed to use the software, etc.) *is vulnerable to at least one accurately identified vulnerability* (e.g., one of a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *based on the identified at least one configuration* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.)*, utilizing the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) *that is used to identify the plurality of potential vulnerabilities* (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: Each node has "AMP for Endpoints" Connector software installed thereon that identifies the operating system/applications/versions thereof on such node and, based thereon, uses the second vulnerability information (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) to identify the plurality of

Claim 1 Elements	Applicability
	potential vulnerabilities (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.). "Whenever an executable file is moved, copied, or executed the AMP for Endpoints Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database that information is displayed on the Vulnerable Software page. Currently the following applications and versions on Windows operating systems are reported on the vulnerabilities page: ... By default, all known vulnerable programs are shown. ... Additional information is available at the bottom of the expanded program list item. The following topics provide additional information through the associated links: • Observed in Groups • Last Observed (computer) • Events • File Trajectory" Cisco *AMP for Endpoints User Guide*, Chapter 20, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more network monitors;	Cisco Advanced Malware Protection (AMP) is configured to *identify an occurrence* (e.g., a discrete event that triggers at least one of the signature/policy updates for the anti-virus, intrusion detection, and/or firewall software, etc.) *in connection with at least one of the plurality of devices*

Claim 1 Elements	Applicability
	(e.g., one of the 50+ nodes licensed to use the software, etc.)*, utilizing one or more network monitors* (e.g., Cisco AMP for Endpoints Connector, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**Correlate discrete events into coordinated attacks**: Cisco AMP for Networks illustrates the risk associated with an ongoing attack. It provides automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources." https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added) **Note**: As set forth below, the "AMP for Endpoints" Connector software installed on user nodes is a dedicated network monitoring application. "**File and Process Scan** **Monitor File Copies** and Moves is the ability for the AMP for Endpoints Connector to give real-time protection to files that are copied or moved. **Monitor Process Execution** is the ability for the AMP for Endpoints Connector to give real-time protection to files that are executed. **Verbose History** (Windows Connector 5.1.9 or higher only) controls whether or not Windows Connectors will write verbose history information to the history.db file. **On Execute Mode** can run in two different modes: Active or Passive. In Active mode, files and scripts are blocked from being executed until a determination of whether or not it is malicious or

Claim 1 Elements	Applicability
	a timeout is reached. In Passive mode, files and scripts are allowed to be executed and in parallel the file is looked up to determine whether or not it is malicious. **WARNING**! Although Active mode gives you better protection, it can cause performance issues. If the endpoint already has an antivirus product installed it is best to leave this set to Passive. **Maximum Scan File Size** limits the size of files that are scanned by the AMP for Endpoints Connector. Any file larger than the threshold set will not be scanned. **Maximum Archive Scan File Size** limits the size of archive files that are scanned by the AMP for Endpoints Connector. Any archive file larger than the threshold set will not be scanned." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
based on a packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and	Cisco Advanced Malware Protection (AMP) is configured to, *based on a packet analysis* (i.e., inspecting incoming and outgoing network communications to prevent threats, etc.)*, determine that the at least one accurately identified vulnerability* (e.g., one of the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one of the plurality of devices* (e.g., one of the 50+ nodes licensed to use the software, etc.) *is susceptible to being taken advantage of by the occurrence* (e.g., the discrete event that triggers at least one of the signature/policy updates for the anti-virus, intrusion detection, and/or firewall software, etc.) *identified in connection with the at least one of the plurality of devices* (e.g., one of the 50+ nodes licensed to use the software, etc.)*, utilizing the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof)*; and*

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any): **Note**: The TETRA/ClamAV anti-virus software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device's operating system) trigger a response. "**TETRA** TETRA is a full antivirus replacement and should never be enabled if another antivirus engine is installed. TETRA can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment. To enable TETRA and adjust settings go to **Advanced Settings > TETRA** in your policy." Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**Detection Engines** Windows, Mac, and Linux Connectors have the option of enabling offline detection engines (**TETRA** for Windows and **ClamAV** for Mac and Linux) to protect the endpoint from malware without connecting to the Cisco Cloud to query each file." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

Claim 1 Elements	Applicability
	Note: The anti-intrusion software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device's operating system) trigger a response. "**Detect and Block Exploit Attempts** Cisco AMP for Networks builds on the Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS). When the system is deployed in line, it detects and blocks client-side exploit attempts that can lead to malicious file downloads, commonly referred to as drive-by attacks. The NGIPS system can also protect against other vulnerability exploit attempts aimed at web browsers, Adobe Acrobat, Java, Flash, and other commonly targeted client applications. Acting as early as possible in the attack chain, the system attempts to limit collateral damage and avoid costly cleanup efforts." https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (emphasis added) "**Exploit Prevention** (Connector version 6.0.5 and later) The AMP for Endpoints Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a **Custom Detections - Simple** list. To enable the exploit prevention engine, go to Modes and Engines in your policy and select Audit or Block mode. Audit mode is only available on AMP for Endpoints Windows Connector 7.3.1 and later. Earlier versions of the Connector will treat Audit mode the same as Block mode."

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "AMP for Endpoints Premier subscriptions include Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco AMP Efficacy Research Team to help identify threats found within the customer environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation. ... **Remediation** includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable." Cisco *AMP for Endpoints User Guide*, Chapter 28, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**AMP for Endpoints Exploit Prevention** ...- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy." Chapter 1, (https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf) Last Updated: April 2020 **Note**: The firewall software includes signatures/policies that are triggered by some events, and that are not triggered by other events, so that only malicious events (relevant to the device's operating system) trigger a response.

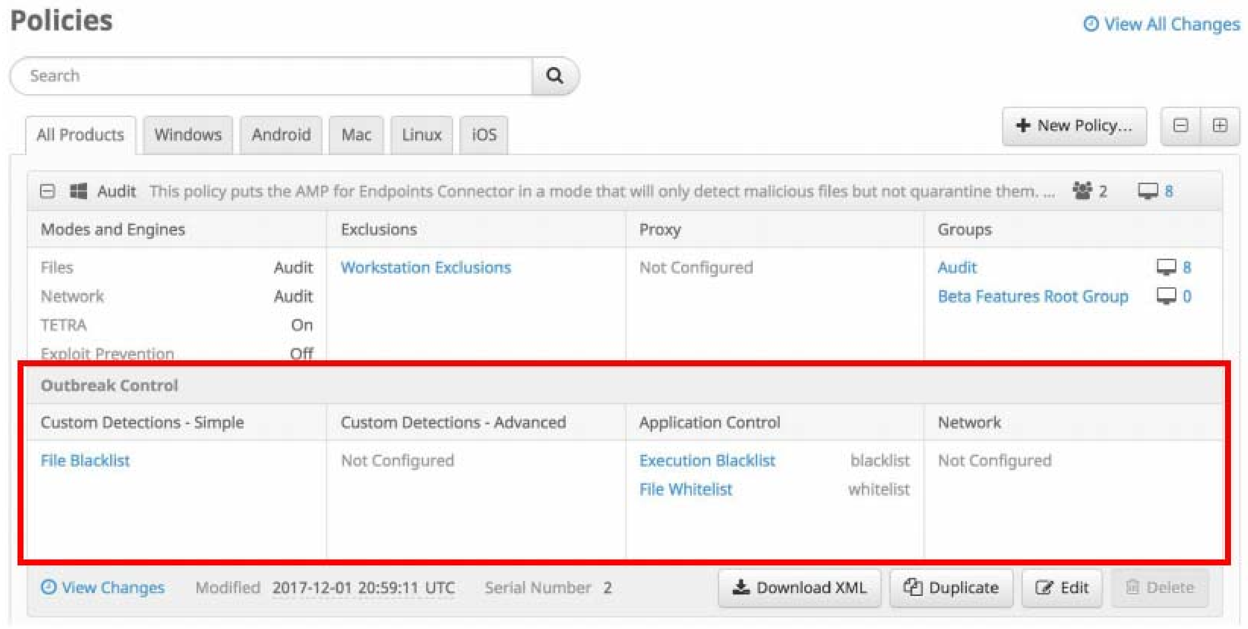
Claim 1 Elements	Applicability
	“**Firewall Connectivity** To allow the AMP for Endpoints Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are three sets of servers depending on where you are located: one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world. IMPORTANT! If your firewall requires IP address exceptions, see this Cisco TechNote.” Cisco *AMP for Endpoints User Guide*, Chapter 7, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 “**AMP for Endpoints Windows Connector 7.0.5** New • Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. • System Process Protection notifications • are less verbose. (CSCvn41948) • are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)” Cisco *AMP for Endpoints Release Notes*, October 8, 2019 Update (https://docs.amp.cisco.com/Release%20Notes.pdf)
allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a	Cisco Advanced Malware Protection (AMP) is configured to *allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types* (e.g., firewall software-, intrusion detection software-, anti-virus software-related actions, etc.), *including a firewall-based occurrence mitigation type* (e.g., firewall software-related actions including quarantining and/or

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;	blocking, etc.) *and an intrusion prevention system-based occurrence mitigation type* (e.g., intrusion detection related actions including detecting and blocking client-side exploit attempts that can lead to malicious file downloads, etc.)*, across the plurality of devices* (e.g., one of the 50+ nodes licensed to use the software, etc.) *for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities* (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types* (e.g., firewall software-, intrusion detection software-, anti-virus software-related actions, etc.) *across the plurality of devices* (e.g., the 50+ nodes licensed to use the software, etc.)*;* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**Policy Summary** Click on a policy to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons at the top right of the list to do the same for all the policies on the page.

PRELIMINARY INFRINGEMENT CLAIM CHART

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	

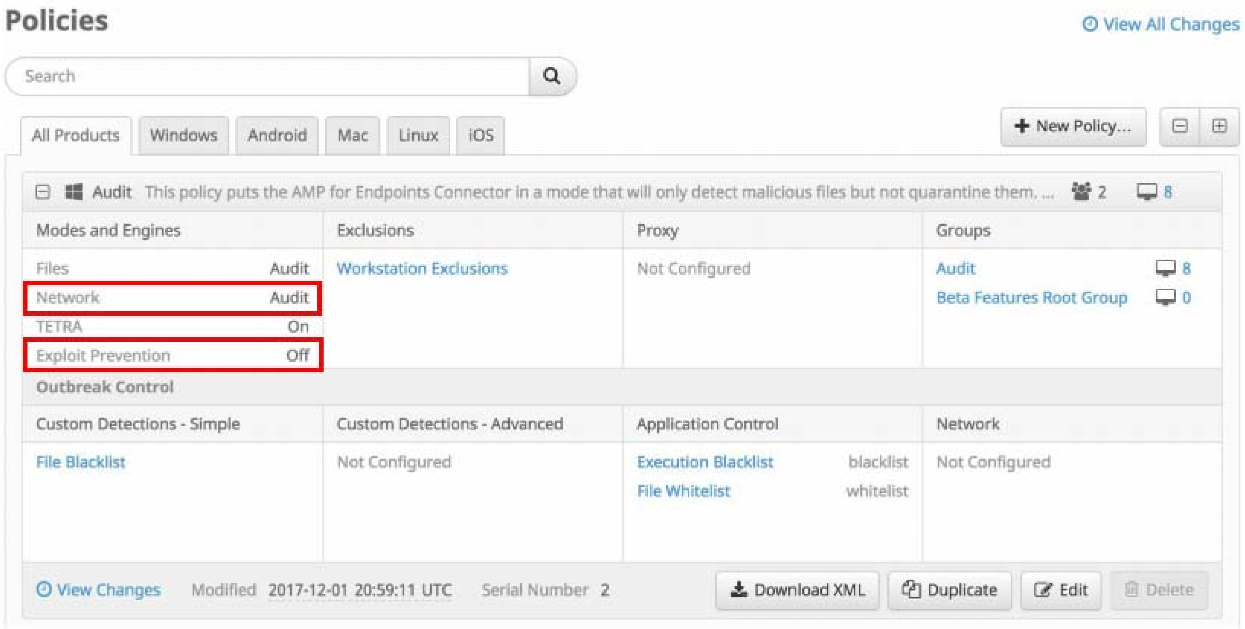
Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 2 8

Modes and Engines	Exclusions	Proxy	Groups
Files Audit Network Audit TETRA On Exploit Prevention Off	Workstation Exclusions	Not Configured	Audit 8 Beta Features Root Group 0

Outbreak Control

Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
File Blacklist	Not Configured	Execution Blacklist blacklist File Whitelist whitelist	Not Configured

Modified 2017-12-01 20:59:11 UTC Serial Number 2

Claim 1 Elements	Applicability
	 Policies View All Changes Search All Products · Windows · Android · Mac · Linux · iOS New Policy... Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 2 8 Modes and Engines: Files Audit; Network Audit; TETRA On; Exploit Prevention Off Exclusions: Workstation Exclusions Proxy: Not Configured Groups: Audit 8; Beta Features Root Group 0 Outbreak Control Custom Detections - Simple: File Blacklist Custom Detections - Advanced: Not Configured Application Control: Execution Blacklist blacklist; File Whitelist whitelist Network: Not Configured View Changes Modified 2017-12-01 20:59:11 UTC Serial Number 2 Download XML · Duplicate · Edit · Delete **View Changes** will take you to a filtered view of the Audit Log showing all the changes for that specific policy. You can also use **View All Changes** at the top of the page to show changes to all policies. Click **Edit** to modify an existing policy or click **Duplicate** if you want to create a new policy with the same settings." Cisco *AMP for Endpoints User Guide*, Chapter 4, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020 "**Outbreak Control**

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 1 Elements	Applicability
	The **Outbreak Control** menu contains items related to controlling outbreaks in your network. • Custom Detections o Simple to convict files that are not yet classified. o Advanced to create signatures that will detect parts of the Portable Executable (PE) file. o Android to warn of new threats or unwanted apps. • Application Control o Blocked Lists to stop executables from running. o Allowed Lists to create lists of applications that will not be wrongly detected. • Network o IP Blocked & Allowed Lists allow you to explicitly detect or allow connections to specified IP addresses. • Endpoint IOC o Initiate Scan to schedule and start IOC scans on your AMP for Endpoints Connectors (Administrator only). o Installed Endpoint IOCs to upload new endpoint IOCs and view installed endpoint IOCs (Administrator only). o Scan Summary to view the results of endpoint IOC scans. • Automated Actions o Automated Actions lets you set actions that automatically trigger when a specified event occurs on a computer." Cisco *AMP for Endpoints User Guide*, Chapter 1, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020
wherein the at least one configuration involves at least one operating system.	Cisco Advanced Malware Protection (AMP) is configured *wherein the at least one configuration* (e.g., the Windows, Mac, Linux, and/or Android operating system, etc., or an application/version thereof, etc.) *involves at least one operating system.*

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

“**Vulnerabilities**

Vulnerabilities are displayed through a heat map that shows groups that include computers with known vulnerable applications installed.”
Cisco *AMP for Endpoints User Guide*, Chapter 1, (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf) Last Updated: December 14, 2020

“Deployment Options for Protection Everywhere

Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:”

<table>
<tr><th>Product Name</th><th>Details</th></tr>
<tr><td>Cisco AMP for Endpoints</td><td>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.</td></tr>
</table>

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html (emphasis added)

“**Software requirements**”

</td></tr>
</table>

Patent No. 10,609,063, Claim 1: Cisco Advanced Malware Protection (AMP) for Endpoints

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Cisco AMP for Endpoints</td><td><ul><li>Microsoft Windows XP with Service Pack 3 or later</li><li>Microsoft Windows Vista with Service Pack 2 or later</li><li>Microsoft Windows 7</li><li>Microsoft Windows 8 and 8.1</li><li>Microsoft Windows 10</li><li>Microsoft Windows Server 2003</li><li>Microsoft Windows Server 2008</li><li>Microsoft Windows Server 2012</li><li>Mac OS X 10.7 and later</li><li>Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3</li><li>Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3</li></ul></td></tr>
<tr><td>Cisco AMP for Endpoints on Android mobile devices</td><td>Android version 2.1 and later</td></tr>
<tr><td>Cisco AMP for Endpoints on Apple iOS</td><td>MDM supervised iOS version 11</td></tr>
</table>
https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html
</td></tr>
</table>

Caveat: The notes and/or cited excerpts utilized herein are set forth for illustrative purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same in connection with any subsequent correlations.